

597 30-65
M/4t

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

#2

10-825 U.S. PTO
09/729836

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application:

1999年12月 7日

出願番号
Application Number:

平成11年特許願第347562号

出願人
Applicant(s):

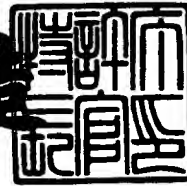
株式会社デンソー

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年11月17日

特許庁長官
Commissioner,
Patent Office

及川耕造



出願番号 出願特2000-3095841

【書類名】 特許願

【整理番号】 PNID3242

【提出日】 平成11年12月 7日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 9/06

【発明者】

 【住所又は居所】 愛知県刈谷市昭和町 1 丁目 1 番地 株式会社デンソー内

 【氏名】 菅沼 武史

【発明者】

 【住所又は居所】 愛知県刈谷市昭和町 1 丁目 1 番地 株式会社デンソー内

 【氏名】 藤井 義光

【発明者】

 【住所又は居所】 愛知県刈谷市昭和町 1 丁目 1 番地 株式会社デンソー内

 【氏名】 穂塚 稔

【特許出願人】

 【識別番号】 000004260

 【氏名又は名称】 株式会社デンソー

【代理人】

 【識別番号】 100082500

 【弁理士】

 【氏名又は名称】 足立 勉

 【電話番号】 052-231-7835

【手数料の表示】

 【予納台帳番号】 007102

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

特平 1 1 - 3 4 7 5 6 2

【包括委任状番号】 9004766

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 電子制御装置の制御情報書換システム

【特許請求の範囲】

【請求項 1】

車両を制御するために車載され、前記制御のための制御情報を電氣的に書き換え可能な不揮発性メモリに記憶した電子制御装置と、

前記制御情報を書き換えるための書換装置とを備え、

前記書換装置は、所定のアクセス情報を用いた通信開始処理を前記電子制御装置との間で実行し、

一方、前記電子制御装置は、前記通信開始処理によって前記書換装置の正当性を判断し、当該書換装置が正当であると判断すると、前記書換装置から送信される変更データに基づき前記制御情報の一部又は全部を書き換える制御情報書換システムにおいて、

さらに、前記書換装置との間でデータ通信を行うセンタを備え、

前記センタは、

前記所定のアクセス情報、前記書換装置の識別情報及び当該識別情報に対応する対応情報を記憶した記憶手段と、

前記書換装置とのデータ通信において、当該書換装置の識別情報及び対応情報を取得し、当該取得した情報の対応関係が前記記憶手段に記憶された対応関係と一致している場合は、前記記憶手段に記憶された前記アクセス情報を前記書換装置へ送信し、一方、一致していない場合は、前記アクセス情報を前記書換装置へ送信しない正当性判断手段とを有すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 2】

請求項 1 に記載の制御情報書換システムにおいて、

前記書換装置は、前記アクセス情報として電子制御装置に記憶された関数 F に対応する関数 f を前記センタから取得し、前記電子制御装置から送信される所定値 r に対する関数値 $f(r)$ を電子制御装置に送信し、

一方、電子制御装置は、前記書換装置から送信される関数値 $f(r)$ に対する

関数値 $F(f(r))$ が前記送信した所定値 r に等しければ、前記書換装置が正当であると判断すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 3】

請求項 2 に記載の制御情報書換システムにおいて、

前記所定値 r は、前記電子制御装置にて生成される乱数であること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 4】

請求項 1 ～ 3 のいずれかに記載の制御情報書換システムにおいて、

前記電子制御装置は、前記書換装置が正当でないと所定回数判断すると、前記書換装置からのアクセスを一定時間拒否すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 5】

請求項 1 ～ 4 のいずれかに記載の制御情報書換システムにおいて、

前記対応情報は、前記センタとのデータ通信可能状態が確立される毎に、利用者によって前記書換装置へ入力され、

前記書換装置は、前記識別情報と共に前記利用者によって入力された前記対応情報を前記センタへ送信すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 6】

請求項 1 ～ 4 のいずれかに記載の制御情報書換システムにおいて、

前記センタと前記書換装置との間に電話回線を介してデータ通信可能状態が確立されるよう構成されており、

前記センタは、前記データ通信可能状態が確立されると、前記書換装置側の電話番号を前記対応情報として取得すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 7】

請求項 1 ～ 6 のいずれかに記載の制御情報書換システムにおいて、

前記センタは、前記正当性判断手段にて前記対応関係の不一致が所定回数判断

されると、前記書換装置からのアクセスを一定時間拒否すること
を特徴とする電子制御装置の制御情報書換システム。

【請求項 8】

請求項 1 ～ 7 のいずれかに記載の制御情報書換システムにおいて、
前記センタは、

さらに、前記制御情報の変更データを記憶する変更データ記憶手段を有しており、

前記電子制御装置にて前記書換装置が正当であると判断された場合に、変更情報記憶手段に記憶された変更データを前記書換装置へ送信すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 9】

請求項 8 に記載の制御情報書換システムにおいて、

前記電子制御装置は、前記書換装置が正当であると判断すると、前記車両を特定するための車両情報を書換装置へ送信し、

前記センタは、

さらに、前記車両に係る前記制御情報の更新履歴を記憶する更新履歴記憶手段を有しており、

前記電子制御装置からの前記車両情報が前記書換装置によって送信されると、当該車両情報に基づき前記更新履歴記憶手段に記憶された更新履歴を参照し、当該車両において前記制御情報の書き換えの必要性を判断し、書き換えが必要であると判断すると、前記変更データ記憶手段に記憶された変更データを前記書換装置へ送信すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 1 0】

請求項 1 ～ 9 のいずれかに記載の制御情報書換システムにおいて、

前記センタは、前記電子制御装置にて前記制御情報の書き換えが完了すると、前記更新履歴記憶手段に記憶された、当該電子制御装置が搭載された車両に対する前記更新履歴を更新すること

を特徴とする電子制御装置の制御情報書換システム。

【請求項 1 1】

請求項 1 ～ 1 0 のいずれかに記載の制御情報書換システムにおいて、
前記書換装置は、前記電子制御装置にて前記制御情報の書き換えが完了すると、
前記所定のアクセス情報を抹消すること
を特徴とする電子制御装置の制御情報書換システム。

【請求項 1 2】

請求項 1 ～ 1 1 のいずれかに記載の制御情報書換システムにおいて、
前記書換装置と前記センタとの間でデータ通信可能状態が確立された後、前記
電子制御装置にて前記制御情報の書き換えが完了する前に前記書換装置と前記セ
ンタとの間のデータ通信が不能となった場合、前記書換装置が前記制御情報の書
き換えを中止すること
を特徴とする電子制御装置の制御情報書換システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、電氣的にデータの書き換えが可能な不揮発性メモリを有する電子制
御装置（以下「ECU」ともいう。）に関し、特に当該不揮発性メモリに記憶さ
れた制御プログラムや制御データといった制御情報の不正な書き換えを防止する
技術に関する。

【0 0 0 2】

【従来の技術】

従来より、自動車のエンジン等を制御する ECU には、電氣的にデータの書き
換えが可能な不揮発性メモリに制御情報を格納したものがある。ここで制御情報
とは、制御用のプログラム及びデータをいう。これによって、このような制御情
報を、市場への供給後でも書き換え可能にしている。

【0 0 0 3】

すなわち、この種の ECU は、通常時には、不揮発性メモリに格納された制
御情報に従ってエンジン等の制御対象を制御するための制御処理を実行するのであ
るが、別途用意された書換装置が接続されて、その書換装置から書き換え指令が

送信されて来ると、所定の通信手順を踏んだ後に、不揮発性メモリの内容を書き換えるように構成されている。なお、不揮発性メモリの内容の書き換えは、不揮発性メモリに格納されている制御情報の一部又は全部を消去し、その消去したメモリ領域に、メモリ書換装置から送信されてくる変更データとしての新たな制御情報を書き込むという手順で行われる。

【0004】

具体的には図9に示すように、車両100に用意された車両ダイアグコネクタ120を介して書換装置200が接続される。図9では、車両100に4つのECU101, 102, 103, 104が搭載されており、各ECU101~104は、ネットワーク回線110にて結ばれている。書換装置200は、作業者による操作に基づきECUコードを送信することによって、4台のECU101~104のうちの1台とデータ通信を行う。

【0005】

このようなECUでは、不揮発性メモリに格納される制御情報を書換装置を用いて書き換えることができるため、動作内容（制御内容）を任意に変更することができるという点で有利である。特に、動作内容（制御内容）に不具合があった場合も迅速に対応できることになり、市場への供給後における車両のメンテナンスを容易にする。

【0006】

しかしその反面、利用者が制御情報を故意に書き換える可能性が残される。すなわち、環境面や安全面を配慮して設定される制御情報を、利用者が快適性や興味などで書き換えてしまう可能性がある。例えば、エンジンを制御するECUでは、車速の上限値を制御データとして予め設定しておき、車速がその上限値を越えた場合には、燃料をカットするというような安全面からの制御を行うのが一般的である。このとき、利用者が、予め設定された車速の上限値（制御データ）を故意に書き換えることが考えられる。このように制御情報が利用者によって故意に書き換えられると、環境面や安全面において妥当でない状況が発生する。

【0007】

そのため、E-OBDの電子システムセキュリティ規定で不正な制御情報の書

き換えを防止することが義務付けられている。そこで次に、従来の書換処理を図面を用いて説明する。

図 10 の左側に示した処理が図 9 における ECU 101～104 の処理に相当し、図 10 の右側に示した処理が図 9 における書換装置 200 の処理に相当している。なお、各処理には b1～b12 の符号を付した。以下、この符号を用いて処理の説明を行う。

【0008】

まず最初に書換装置が制御情報の書き換えを行う ECU を選択し、書換要求を送信する (b1)。ECU の選択は、ECU コードを送信することによって行う。この ECU コードは作業者によって書換装置に入力される。すると、選択された ECU は、乱数 r を発生し (b2)、この乱数 r を書換装置へ送信する (b3)。

【0009】

書換装置には関数 f が予め記憶されており、送信される乱数 r に対して関数値 $f(r)$ を算出する (b4)。そして、その算出した関数値 $f(r)$ を送信する (b5)。一方、ECU には関数 F が予め記憶されており、送信される関数値 $f(r)$ に対して関数値 $F(f(r))$ を算出する (b6)。続いて、算出した $F(f(r))$ が乱数 r に等しければ、すなわち $f = F^{-1}$ であれば、書き換えを許可する許可信号を送信する (b7)。

【0010】

ここまでの処理は、ECU が記憶する関数 F の逆関数 f を書換装置が有している場合に、ECU が書換装置を正当であると判断するものである。この例では、書換装置の有する関数 f が ECU をアクセスするための情報となっている。

書換装置は、ECU から送信される許可信号を受信すると (b8)、変更データを送信する (b9)。ECU は、この変更データに基づき制御情報の書き換えを行う (b10)。

【0011】

ECU は制御情報の書き換えが正常に終了すると、正常終了を通知し (b11)、書換装置が通知を受けて (b12) 一連の書き換え処理が完了する。

【0 0 1 2】

【発明が解決しようとする課題】

図 1 0 を用いて説明した書換処理では、書換装置内の情報である関数 f を用いた通信処理（b 1 ～ b 7）によって、E C U が書換装置の正当性を判断している。そのため、書換装置自体が盗まれたり、又は、書換装置内部の情報が盗まれたりした場合には、不正な制御情報の書き換えを防止できないという問題があった。特に、書換装置は作業現場にあるため、上述した盗難の可能性が比較的高くなってしまう。

【0 0 1 3】

本発明は、上述した問題点を解決するためになされたものであり、書換装置又は書換装置内部の情報が盗まれた場合であっても、上述した不正な制御情報の書き換えを防止できるようにすることを目的とする。

【0 0 1 4】

【課題を解決するための手段及び発明の効果】

上述した目的を達成するためになされた請求項 1 に記載の制御情報書換システムは、車両を制御するために車載され、制御のための制御情報を電氣的に書き換え可能な不揮発性メモリに記憶した電子制御装置と、制御情報を書き換えるための書き換え装置とを備えることを前提としている。

【0 0 1 5】

このとき、書換装置は、所定のアクセス情報を用いた通信開始処理を電子制御装置との間で実行し、一方、電子制御装置は、通信開始処理によって書換装置の正当性を判断し、当該書換装置が正当であると判断すると、書換装置から送信される変更データに基づき制御情報の一部又は全部を書き換える。

【0 0 1 6】

このような構成に加え、本発明のシステムではさらに、書換装置との間でデータ通信を行うセンタを備えていることを特徴としている。センタは、例えば作業現場とは別の場所に設置されることが考えられる。

このセンタの記憶手段には、上述したアクセス情報が記憶されている。また、書換装置の識別情報及び対応情報が記憶されている。識別情報は、書換装置を識

別するための書換装置固有の番号などであることが考えられる。一方、対応情報は、各識別情報に対応させて設定される情報である。

【 0 0 1 7 】

センタの正当性判断手段は、書換装置とのデータ通信において、当該書換装置の識別情報及び対応情報を取得する。そして、当該取得した情報の対応関係が記憶手段に記憶された対応関係と一致している場合は、所定のアクセス情報を書換装置へ送信する。一方、一致していない場合は、所定のアクセス情報を書換装置へ送信しない。

【 0 0 1 8 】

つまり、本発明では、電子制御装置へのアクセスを可能にするアクセス情報を、書換装置ではなくセンタに記憶しておき、書換装置が正当であることをセンタが判断した場合に、センタからアクセス情報を送信する。

これは、以下のような２段階のチェックを行うことにあたる。

【 0 0 1 9 】

①センタが書換装置の正当性を判断してアクセス情報を書換装置へ送信する。

②書換装置はそのアクセス情報を用いた通信開始処理を実行し、その通信開始処理に基づき、電子制御装置が書換装置の正当性を判断する。

上記①の段階の正当性判断を、識別情報と対応情報との対応関係で行う。

【 0 0 2 0 】

これによって、少なくとも識別情報又は対応情報のいずれか一方を書換装置内部に記憶しておかなければ、上記①の段階で書換装置はセンタからアクセス情報を得ることができない。したがって、書換装置又は書換装置内部の情報が盗まれたとしても、上記②において電子制御装置により書換装置が正当であると判断されないため、その後、制御情報の書き換えが行われない。その結果、書換装置や書換装置内の情報が盗まれた場合であっても、電子制御装置の制御情報が不正に書き換えられることを防止できる。

【 0 0 2 1 】

ところで、上記②における「アクセス情報を用いた通信開始処理」とは、従来技術として既に述べた従来と同様の処理とすることが一例として考えられる。す

なわち、請求項 2 に示す構成とすることが考えられる。

この場合は、書換装置が、電子制御装置に記憶された関数 F に対応する関数 f をアクセス情報としてセンタから取得し、電子制御装置から送信される所定値 r に対する関数値 $f(r)$ を電子制御装置に送信する。一方、電子制御装置は、書換装置から送信される関数値 $f(r)$ に対する関数値 $F(f(r))$ が送信した所定値 r に等しければ、すなわち、 $F = f^{-1}$ ($f = F^{-1}$) であれば書換装置が正当であると判断する。なお、所定値 r は固定的なものとしてもよいが、請求項 3 に示すように、乱数を用いることが考えられる。

【0022】

なお、正当なアクセス情報を得ることなく、書換装置による電子制御装置への不正なアクセスが行われることを防止するために、請求項 4 に示す構成を採用してもよい。この構成では、電子制御装置が、書換装置を正当でないと所定回数判断すると、書換装置からのアクセスを例えば 10 分というような一定時間拒否する。所定回数は 1 回としてもよいが、通信エラーなどが生じる可能性を考慮して例えば 3 回というように設定することが考えられる。また、所定回数は、「正当でない」という判断が連続して行われた回数であってもよいし、「正当でない」という判断を累積した回数としてもよい。このようにすれば、不正なアクセス情報を用いては連続的に何度も電子制御装置をアクセスすることができないため、不正な電子制御装置へのアクセスを効果的に防止することができ、制御情報の書き換え防止に有効である。

【0023】

ところで、上記④における書換装置の正当性判断において、センタは、書換装置の識別情報及び対応情報の対応関係を利用している。

したがって、上述したように、識別情報又は対応情報の少なくともいずれか一方を書換装置内部に記憶しておかなければ、書換装置又は書換装置内部の情報が盗まれた場合であっても、書換装置はセンタからアクセス情報を得ることはできない。

【0024】

そこで、例えば請求項 5 に示すように、少なくとも対応情報は、センタとのデ

ータ通信可能状態が確立する度に、利用者によって書換装置へ入力されるようにするとよい。このとき、書換装置は、識別情報と共に、利用者によって入力された対応情報をセンタへ送信する。

【 0 0 2 5 】

ここでいう対応情報は、識別情報に対応するいわゆるパスワードとして位置付けられる。このように毎回利用者が対応情報を入力するようにすれば、書換装置又は書換装置内の情報が盗まれ識別情報が盗まれたとしても、それに対応する対応情報が分からないため、センタからアクセス情報を得ることができない。したがって、電子制御装置の制御情報が不正に書き換えられることを防止できる。

【 0 0 2 6 】

なお、「少なくとも対応情報」としたのは、上述したように識別情報も、書換装置内部に記憶しておかず、例えば対応情報と同様に利用者によって入力されるようにしてもよいためである。その場合、利用者が入力する情報は増えるものの、書換装置又は書換装置内部の情報が盗まれた場合に対応情報だけでなく識別情報までも分からないため、センタからアクセス情報を不正に得られる可能性がさらに低くなり、制御情報が不正な書き換えに対して有効となる。

【 0 0 2 7 】

ただし、対応情報があるいは識別情報と対応情報とを利用者が入力する上述の構成を採用しても、それらの情報が何らか別のルートで盗まれる可能性も考えられる。そこで、請求項 6 に示す構成を採用することが考えられる。

この構成は、センタと書換装置との間に電話回線を介してデータ通信可能状態が確立されることを前提とする。センタは、書換装置との間にデータ通信可能状態が確立されると、書換装置側の電話番号を対応情報として取得する。このとき、センタは、取得される識別番号と電話番号との対応が記憶手段に予め記憶された対応と一致するか否かを判断し、一致すればアクセス情報を送信する。

【 0 0 2 8 】

このようにすれば、別の場所、すなわち正規の作業場所以外からセンタとの間に回線を接続した場合、センタの取得する対応情報としての電話番号は予め決められた電話番号でなくなる。そのため、識別情報と対応せず、センタからアクセ

ス情報を得ることはできない。つまり、この技術思想は、不正な書き換えが行われる場合には書換装置が正規の設置場所でない、という事実に着目したものである。このようにすれば、書換装置や書換装置内の情報が盗まれた場合であっても、電子制御装置の制御情報が不正に書き換えられることを確実に防止できる。

【0029】

ところで、電子制御装置にて書換装置が正当でないと判断された場合に、電子制御装置が書換装置からのアクセスを例えば10分というような一定時間拒否することによって、電子制御装置への不正なアクセスが効果的に防止できることは上述した。センタと書換装置との間にも、同様の手法を採用することが考えられる。

【0030】

すなわち請求項7に示すように、センタは、正当性判断手段にて対応関係の不一致が所定回数判断された場合、書換装置からのアクセスを一定時間拒否するようにするとよい。ここでいう「所定回数」の意味するところは、既に述べた請求項3に記載の所定回数と同様であるため省略する。このようにすれば、センタへの不正なアクセスを連続して何度も行うことができない。したがって、不正な制御情報の書き換えを防止するのに有効である。

【0031】

ところで従来は、書換装置の有する記録媒体に制御情報を書き換えるための変更データを記憶していた。本発明においても、変更データを書換装置に記憶する構成としてもよい。しかし、さらにセキュリティ面を考慮するならば、請求項8に示すような構成を採用することが望ましい。

【0032】

この構成では、センタが、さらに、制御情報の変更データを記憶する変更データ記憶手段を有しており、電子制御装置にて書換装置が正当であると判断された場合に、変更情報記憶手段に記憶された変更データを書換装置へ送信する。

この場合は、書換装置でなくセンタに変更データを記憶しておく。これによって、書換装置又は書換装置内部の情報が盗まれた場合であっても、変更データが外部に漏れる可能性がない。さらに、上記②において書換装置が正当であるとの

判断がなされた後に、変更データを書換装置へ送信する。もちろん、上記①において書換装置の正当性をセンタが判断した場合に、アクセス情報と共に変更データを書換装置へ送信するようにしてもよい。しかし、上述したように電子制御装置にて書換装置が正当であると判断された場合に変更データを送信するようにすれば、すなわち、上記①及び②のチェックが行われた後に変更データを送信するようにすれば、さらにセキュリティ面で有利である。

【 0 0 3 3 】

なお、この場合には、電子制御装置が書換装置を正当なものであると判断すると、書き換えの許可を示す情報を電子制御装置が書換装置へ送信し、さらに、書換装置がこの情報をセンタに送信することによって、センタが変更データを送信するという具合である。

【 0 0 3 4 】

このような構成を前提としてさらなる工夫をすれば、次に示すような問題を解決することができる。

その問題とは、従来、過去に電子制御装置の制御情報が書き換えられているか否かを判断できない状況があったことである。

【 0 0 3 5 】

例えば制御プログラムが複数回バージョンアップされているような場合、ある車両に対して同一ユーザが同一の修理工場を利用する場合は、修理工場側で記録を残すことなどで車両の制御プログラムがどこまでバージョンアップされたかを把握することができる。

【 0 0 3 6 】

しかし、車両のユーザが途中で変わった場合や別の修理工場へ車両の点検を依頼した場合などは、制御プログラムのバージョンアップの履歴がないため、既に制御プログラムの書き換えが行われているにもかかわらず、再度制御プログラムの書き換えを行うというような無駄な制御情報の書き換えが行われる状況があった。このような場合、無駄な作業時間を要するだけでなく、例えば制御情報の記憶に E E P R O M を用いている場合、書き換え可能回数が制限されるため、無駄な書き換えによって必要な書き換えができなくなるおそれもあった。

【 0 0 3 7 】

そこで、請求項 9 に示すように、請求項 8 に示した構成に加え、センタが、さらに、車両に係る制御情報の更新履歴を記憶する更新履歴記憶手段を有する構成とすることが考えられる。この場合、電子制御装置は、書換装置が正当であると判断すると、車両を特定するための車両情報を送信する。センタは、電子制御装置からの車両情報が書換装置によって送信されると、当該車両情報に基づき更新履歴記憶手段に記憶された更新履歴を参照する。そして、参照した更新履歴に基づき、当該車両における制御情報の書き換えの必要性を判断し、書き換えが必要であると判断すると、変更データ記憶手段に記憶された変更データを書換装置へ送信する。なお、車両情報は、電子制御装置の搭載された車両を特定するための情報であり、例えば各車両固有の車両 V I N (Vehicle ID Number) コードとすることが考えられる。

【 0 0 3 8 】

このようにすれば、センタによって制御情報の更新履歴が管理されるため、無駄な制御情報の書き換えが行われない。その結果、無駄な作業時間がなくなり、また、無駄な書き換えによって必要な書き換えができなくなることもなくなる。

なお、更新履歴は、例えば作業者が制御情報の書き換え完了後にマニュアル操作で更新してもよいが、請求項 1 0 に示すように自動的に更新されるようにすると便利である。

【 0 0 3 9 】

すなわち、センタは、電子制御装置にて前記制御情報の書き換えが完了すると、更新履歴記憶手段に記憶された、当該電子制御装置が搭載された車両に対する更新履歴を更新するようにするとよい。具体的には、電子制御装置が制御情報の書き換えが完了したことを示す情報を書換装置に送信し、書換装置がさらにこの情報をセンタへ送信する。センタは、この情報に基づき、更新履歴を更新するという具合である。このようにすれば、書き換えの終了時に更新履歴が自動的に更新されるため、作業者にとって便利である。

【 0 0 4 0 】

ところで、センタが書換装置の正当性を判断してアクセス情報を送信した後に

、その書込装置からアクセス情報が盗まれる可能性も考えられる。

したがって、請求項 1 1 に示すように、書換装置は、電子制御装置にて制御情報の書き換えが完了すると、所定のアクセス情報を抹消するのが望ましい。具体的には、電子制御装置が制御情報の書き換えが完了したことを示す情報を書換装置へ送信し、この情報に基づき、書換装置がアクセス情報を抹消するという具合である。このようにすれば、書き換えの終了時にアクセス情報が速やかに抹消されるため、一度送信されたアクセス情報が書換装置から盗まれる可能性を低減させることができる。

【0041】

また、上記④において書換装置がセンタからアクセス情報を取得した後、センタと書換装置との間のデータ通信を一時的に終了することが考えられる。ただし、書換装置に送信されたアクセス情報が盗まれ、別の書換装置を用い、このアクセス情報を使用して電子制御装置がアクセスされる可能性がある。

【0042】

したがって、請求項 1 2 に示すように、書換装置とセンタとの間でデータ通信可能状態が確立された後、電子制御装置にて制御情報の書き換えが完了する前に書換装置とセンタとの間のデータ通信が不能となった場合、書換装置が制御情報の書き換えを中止するようにすることが考えられる。

【0043】

この場合、書換装置の正当性判断を含む一連の書き換え処理が終了するまではセンタと書換装置がデータ通信可能状態となっていることを書き換えの条件とするのである。これによって、盗んだアクセス情報を用いて別の書換装置から電子制御装置をアクセスすることができないため、制御情報が不正な書き換えを確実に防止できる。

【0044】

【発明の実施の形態】

以下、本発明を具体化した一実施例を図面を参照して説明する。

図 1 は、実施例の制御情報書換システム 1 の概略構成を示すブロック図である。車両 1 0 には、4 台の ECU 1 1, 1 2, 1 3, 1 4 が搭載されており、各 E

CU11～14はネットワーク回線15で結ばれている。ECU11～14は、不揮発性メモリとしてのEEPROM（不図示）を有しており、書換装置20が接続されていない通常時には、このEEPROMに記憶された制御情報（制御プログラム及び制御データ）に基づき、ネットワーク回線15を介したECU11～14間通信を行って、エンジン等それぞれの制御対象を制御する。

【0045】

そして、ECU11～14の有するEEPROMに記憶された制御情報を書き換えるためのシステムが、本制御情報書換システム1である。

図1では、書換装置20が車両ダイアグコネクタ16を介して各ECU11～14と接続された様子が示されている。車両ダイアグコネクタ16は、書換装置20と各ECU11～14とのネットワーク回線15を介したデータ通信を可能にするため、車両10に用意されたコネクタである。なお、車両10及び書換装置20は、修理工場などの作業現場に設置されている。

【0046】

また、本実施例の制御情報書換システム1では、書換装置20が電話回線網40を介してセンタ30とデータ通信できるようになっている。センタ30は、いわゆるサーバとして作業現場とは別の場所に設置される。そして、このセンタ30の記憶装置（不図示）には、ECU11～14を書換装置20がアクセスするためのアクセス情報、制御情報を書き換える変更データ、書換装置20の正当性を判断するためのデータベース、及び、各車両10の制御情報の更新履歴のデータベースが記憶されている。したがって、この記憶装置が「記憶手段」、「変更データ記憶手段」及び「更新履歴記憶手段」に相当する。

【0047】

書換装置20とセンタ30とは、書換装置20がセンタ30を発呼することによって、書換装置20とセンタ30との間で所定の通信処理が行われてデータ通信が可能な状態となる。なお、図1には、センタ30が1台の書換装置20と接続されていることを示したが、センタ30に対しては、例えば別の作業現場の書換装置が並行して接続されることも考えられる。

【0048】

次に、本制御情報書換システム 1 の動作の概要を図 2 に基づき説明する。

図 2 では、本制御情報書換システム 1 の動作を B 1 ～ B 1 8 の符号を付したブロック単位で示した。詳しくは、各 ECU 1 1 ～ 1 4 における処理を、ECU 側処理として図 2 中の左側の列に、B 5, B 6, B 9, B 1 0, B 1 5, B 1 6 と示した。また、書換装置 2 0 における処理を、書換装置側処理として中央の列に、B 1, B 4, B 7, B 8, B 1 1, B 1 4, B 1 7 と示した。さらに、センタ 3 0 における処理を、センタ側処理として右側の列に、B 2, B 3, B 1 2, B 1 3, B 1 8 と示した。これらの処理は、B 1 → B 2 → B 3 → … → B 1 8 という順序で実行される。

【0049】

最初に書換装置 2 0 がセンタ 3 0 を発呼し、書換装置 2 0 とセンタ 3 0 との間にデータ通信可能状態が確立されると、書換装置 2 0 は、通信開始要求と共に書換装置 2 0 自体を識別させるための「識別情報」としての ID 情報をセンタ 3 0 へ送信する (B 1)。これに対し、センタ 3 0 は、書換装置 2 0 からの ID 情報を受信すると共に、発呼元の電話番号、すなわち、書換装置 2 0 側の電話番号を取得する (B 2)。この電話番号が「対応情報」に相当する。

【0050】

センタ 3 0 は、書換装置 2 0 の ID 情報と書換装置 2 0 に割り当てられた電話番号とを対応させたデータベースを有している。したがって、センタ 3 0 は次に、受信した ID 情報と取得した電話番号との対応関係をデータベースにある対応関係と照合する (B 2)。ここで一致していれば、第 1 許可信号及び関数 f を書換装置 2 0 へ送信する (B 3)。

【0051】

書換装置 2 0 は、ECU 1 1 ～ 1 4 の中から書き換え対象とする ECU を選択し、その ECU へ書換要求を送信する (B 4)。ここでは ECU 1 1 が書き換え対象の ECU として選択されたものとして以下の説明を続ける。

選択された ECU 1 1 は、乱数 r を発生し (B 5)、この乱数 r を書換装置 2 0 へ送信する (B 6)。

【0052】

書換装置 2 0 は、上記 B 3 にてセンタから送信された関数 f を用い、E C U 1 1 からの乱数 r に対して関数値 $f(r)$ を算出する (B 7)。そして、その算出した関数値 $f(r)$ を E C U 1 1 へ再度送信する (B 8)。

一方、E C U 1 1 には関数 F が予め記憶されており、書換装置 2 0 から送信される関数値 $f(r)$ に対し、関数値 $F(f(r))$ を算出する (B 9)。続いて、算出した $F(f(r))$ が乱数 r に等しければ、すなわち $f = F^{-1}$ であれば、書き換えを許可する第 2 許可信号を送信すると共に、車両 V I N コードを送信する (B 1 0)。車両 V I N コードは、車両毎にユニークに付された番号であり、これが上述の「車両情報」に相当する。

【0 0 5 3】

書換装置 2 0 は、E C U 1 1 からの第 2 許可信号及び車両 V I N コードを受信し、これらの情報をさらに、センタ 3 0 へ送信する (B 1 1)。

センタ 3 0 は、各車両それぞれの制御情報の更新履歴をデータベースとして有している。したがって、書換装置 2 0 からの車両 V I N コードに基づき、車両 1 0 の判別を行い、更新履歴のデータベースを参照して、制御情報の書き換え必要性を判断する (B 1 2)。ここで車両 1 0 に対する制御情報の書き換えが必要であると判断すると、変更データを書換装置 2 0 へ送信する (B 1 3)。

【0 0 5 4】

書換装置 2 0 は、センタ 3 0 からの変更データを受信し、この変更データを E C U 1 1 へ送信する (B 1 4)。

E C U 1 1 は、書換装置 2 0 からの変更データに基づき、制御情報の書き換えを行う (B 1 5)。そして、制御情報の書き換えが正常に終了すれば、正常終了を書換装置 2 0 へ通知する (B 1 6)。

【0 0 5 5】

書換装置 2 0 は、E C U 1 1 から正常終了が通知されると、上記 B 3 にてセンタ 3 0 から送信された関数 f を抹消する (B 1 7)。また、センタ 3 0 に正常終了を通知する。これによって、センタ 3 0 は、更新履歴のデータベースを更新する (B 1 8)。

【0 0 5 6】

以上のようにして一連の書き換え処理が完了する。

次に、上述した ECU 側処理、書換装置側処理、及びセンタ側処理の詳細を順に説明する。なお、各処理の説明にあたって適宜図 2 を参照する。

最初に図 3 及び図 4 のフローチャートに基づき、各 ECU 1 1 ~ 1 4 にて実行される ECU 側処理を説明する。なお、この ECU 側処理は、車両 1 0 に車両ダイアグコネクタ 1 6 を介して書換装置 2 0 が接続された状態において、例えば 0 . 2 秒というような所定時間間隔で実行されるものである。

【0057】

まずステップ S 3 0 0 において、書換装置 2 0 からの書換要求があったか否かを判断する。ここで書換要求があったと判断された場合 (S 3 0 0 : YES)、S 3 1 0 へ移行する。一方、書換要求がなかったと判断された場合 (S 3 0 0 : NO)、以降の処理を実行せずに、本 ECU 側処理を終了する。

【0058】

S 3 1 0 では、アクセス拒否タイマが「0」か否かを判断する。アクセス拒否タイマは、後述するように書換装置 2 0 が「正当でない」と所定回数連続して判断された場合に設定されるものである。ここでアクセス拒否タイマが「0」でないと判断された場合 (S 3 1 0 : NO)、S 3 2 0 にてタイマをデクリメントし、さらに変数 C 1 に「0」を代入して、本 ECU 側処理を終了する。変数 C 1 は、書換装置が正当でないと連続して判断された回数を計数するものである。一方、アクセス拒否タイマが「0」であると判断された場合 (S 3 1 0 : YES)、S 3 3 0 へ移行する。

【0059】

S 3 3 0 では、変数 C 1 が「2」以下であるか否かを判断する。ここで C 1 > 2 である場合 (S 3 3 0 : NO)、S 3 4 0 にてアクセス拒否タイマをセットし、本 ECU 側処理を終了する。本実施例では、10 分がセットされる。一方、C 1 ≤ 2 である場合 (S 3 3 0 : YES)、S 3 5 0 へ移行する。

【0060】

S 3 5 0 では、乱数 r を発生し、書換装置 2 0 へ送信する。この処理は、図 2 中の B 5 及び B 6 の処理に相当する。これに対し、図 2 中の B 8 に示したように

、書換装置 2 0 から関数値 $f(r)$ が送信される。

したがって、続く S 3 6 0 では、関数値 $f(r)$ の送信があったか否かを判断する。ここで関数値 $f(r)$ の送信があった場合 (S 3 6 0 : YES)、S 3 7 0 へ移行する。一方、関数値 $f(r)$ の送信がない場合は (S 3 6 0 : NO)、この判断処理を繰り返す。

【0061】

S 3 7 0 では、書換装置 2 0 から送信される関数値 $f(r)$ に対し、関数値 $F(f(r))$ を算出する。この処理は、図 2 中の B 9 の処理に相当する。

続く図 4 の S 3 8 0 では、算出した関数値 $F(f(r))$ が乱数 r に等しいか否かを判断する。ここで $F(f(r)) = r$ である場合 (S 3 8 0 : YES)、S 3 9 0 にて第 2 許可信号及び車両 VIN コードを送信し、S 4 2 0 へ移行する。この S 3 8 0 及び S 3 9 0 の処理が図 2 中の B 1 0 の処理に相当する。一方、 $F(f(r)) \neq r$ である場合 (S 3 8 0 : NO)、書き換えを許可しない旨を S 4 0 0 にて書換装置 2 0 に通知し、S 4 1 0 にて変数 C 1 をインクリメントして、本 ECU 側処理を終了する。このようにして書換装置 2 0 の正当性が判断され、正当でないと判断した場合 (S 3 8 0 : NO) 変数 C 1 がインクリメントされ (S 4 1 0)、上述したように $C 1 > 2$ でタイマがセットされる (図 3 中の S 3 4 0)。したがって、本実施例では、C 1 が「0」→「1」→「2」という具合に、3 回連続して書換装置 2 0 が正当でないと判断されると、アクセス拒否がなされることになる。

【0062】

上述したように、センタ 3 0 にて車両 VIN コードに基づく制御情報の書き換えの必要性判断がなされ、書き換えが必要があればセンタ 3 0 から書換装置 2 0 を経由して変更データが送信される。一方、書き換えが必要でなければ、すなわち、既に制御情報の書き換えがなされている場合には、書き換え済みであることを示す情報がセンタ 3 0 から書換装置 3 0 を経由して送信される。

【0063】

そのため、S 4 2 0 では、書換装置 2 0 からのデータ送信があったか否かを判断する。ここでデータ送信があったと判断された場合 (S 4 2 0 : YES)、S

4 3 0へ移行する。一方、データ送信がないうちは（S 4 2 0 : N O）、この判断処理を繰り返す。

【 0 0 6 4 】

そして、S 4 3 0では、書換装置 2 0から送信されたデータが変更データか否かを判断する。ここで変更データであると判断された場合（S 4 3 0 : Y E S）、S 4 4 0へ移行する。一方、変更データでないと判断された場合（S 4 3 0 : N O）、すなわち、書き換え済みを示す情報が送信された場合には、以降の処理を実行せず、本 E C U側処理を終了する。

【 0 0 6 5 】

S 4 4 0では、送信された変更データに基づき、制御情報の書き換えを行う。続く S 4 5 0では、書き換え後の制御情報のチェックサムを計算する。これは、正常に制御情報が書き換えられたか否かを判断するためである。

そして、次の S 4 6 0では、S 4 5 0にて計算したチェックサムに基づき、制御情報の書き換えが正常に終了したか否かを判断する。ここで正常に終了したと判断された場合（S 4 6 0 : Y E S）、S 4 7 0にて書換装置 2 0へ正常終了を通知し、その後、本 E C U処理を終了する。一方、正常に終了したと判断されなかった場合（S 4 6 0 : N O）、S 4 8 0にて書換装置 2 0へ変更データの再送信を要求し、S 4 2 0からの処理を繰り返す。

【 0 0 6 6 】

続いて図 5 及び図 6 のフローチャートに基づき、書換装置 2 0にて実行される書換装置側処理を説明する。なお、この書換装置側処理は、書換装置 2 0とセンタ 3 0との間にデータ通信可能状態が確立された後、作業者による所定の操作をトリガとして実行されるものである。

【 0 0 6 7 】

まず最初のステップ S 5 0 0において、センタ 3 0に対し、通信開始を要求すると共に予め記憶されている I D情報を送信する。この処理は、図 2 中の B 1 の処理に相当する。

センタ 3 0は、書換装置 2 0が正当なものであると判断すると、第 1 許可信号及び関数 f を送信してくる。

【0068】

したがって、続くS510では、センタ30からの応答があったか否かを判断する。ここでセンタ30からの応答があったと判断された場合（S510：YES）、S520へ移行する。一方、センタ30からの応答がないうちは（S510：NO）、この判断処理を繰り返す。

【0069】

S520では、センタ30の応答が不許可の通知か否かを判断する。ここで不許可の通知であると判断された場合（S520：YES）、センタ30へのアクセスに失敗した旨をS530にてディスプレイなどの表示装置に表示し、その後、S500からの処理を繰り返す。一方、不許可の通知でない場合（S520：NO）、すなわち第1許可信号及び関数fが送信されてきた場合には、S540へ移行する。

【0070】

S540では、車両10に搭載された4台のECU11～14のいずれかを選択するためのECUコードの入力を作業者に要求する。続くS550では、ECUコードの入力があったか否かを判断する。ここでECUコードの入力があったと判断された場合（S550：YES）、S560へ移行する。一方、ECUコードの入力がないうちは（S550：NO）、S540からの処理を繰り返す。なお、ECU11のECUコードが入力されたものとして以下の説明を続ける。

【0071】

S560では、書換要求及びECUコードを送信する。この処理は、図2中のB4の処理に相当する。これによって、入力されたECUコードに対応するECU11が乱数rを発生し、その乱数rを送信してくる（図3中のS350）。

したがって、続くS570では、乱数rが送信されたか否かを判断する。ここで乱数rが送信されたと判断された場合（S570：YES）、S580へ移行する。一方、乱数rが送信されないうちは（S570：NO）、この判断処理を繰り返す。

【0072】

S580では、S510にてセンタ30から送信された関数fを用い、乱数r

に対する関数値 $f(r)$ を算出する。そして次の S590 にて、関数値 $f(r)$ を ECU11 へ送信する。図 2 中の B7 及び B8 の処理に相当する。

これに対して、ECU11 では、図 3 中の S360 にて肯定判断され、関数値 $F(f(r))$ が算出される (S370)。そして、S380 の判断に基づき、第 2 許可信号の送信又は書き換えを許可しない旨の通知を行う (S390, S400)。

【0073】

したがって、続く図 6 中の S600 では、ECU11 の応答があったか否かを判断する。ここで ECU11 の応答があったと判断された場合 (S600: YES)、S610 へ移行する。一方、ECU11 からの応答がないうちは (S600: NO)、この判断処理を繰り返す。

【0074】

S610 では、ECU11 から第 2 許可信号が送信されたか否かを判断する。ここで第 2 許可信号が送信されたと判断された場合 (S610: YES)、S620 にて第 2 許可信号及びその第 2 許可信号と共に送信される車両 VIN コードをセンタ 30 へ送信し、その後、S640 へ移行する。この処理が図 2 中の B11 の処理に相当する。一方、第 2 許可信号が送信されなかった場合 (S610: NO)、すなわち、ECU11 から書き換えを許可しない旨が通知された場合には、S630 にてセンタ 30 に対し不許可となった旨を通知し、その後、図 5 中の S530 へ移行する。

【0075】

S620 にてセンタ 30 に対し第 2 許可信号及び車両 VIN コードを送信すると、上述したようにセンタ 30 は、書き換えの必要性を判断して、書き換えの必要があれば変更データを送信し、一方、書き換えの必要がなければ書き換え済みを示す情報を送信する。

【0076】

したがって、S640 では、センタ 30 の応答があったか否かを判断する。ここでセンタ 30 の応答があったと判断された場合 (S640: YES)、S650 へ移行する。一方、センタ 30 の応答がないうちは (S640: NO)、この

判断処理を繰り返す。

【0077】

S650では、センタ30から送信されたデータが変更データであるか否かを判断する。ここで変更データであった場合（S650：YES）、S680へ移行する。一方、変更データでない場合（S650：NO）、すなわち書き換え済みを示す情報がセンタ30から送信された場合には、関数fを抹消して書き換える必要がない旨を表示し（S660）、書き換え済みを示す情報をECU11へ送信して（S670）、その後、本書換装置側処理を終了する。

【0078】

S680では、センタ30から送信された変更データをECU11へ送信する。この処理は、図2中のB14の処理に相当する。これによって、ECU11では制御情報の書き換えが行われ（図4中のS430：YES、S440）、ECU11から正常終了の通知又は再送信要求がなされる（S470、480）。

【0079】

そこで、次のS690では、ECU11から正常終了の通知があったか否かを判断する。ここで正常終了の通知があったと判断された場合（S690：YES）、関数fを抹消すると共にセンタ30へ正常終了を通知して（S700）、その後、本書換装置側処理を終了する。一方、正常終了の通知がなされない場合（S690：NO）、すなわち変更データの再送信要求がなされた場合には、センタ30へ異常終了を通知し（S710）、本書換装置側処理を終了する。

【0080】

さらに続けて、図7及び図8のフローチャートに基づき、センタ30にて実行されるセンタ側処理を説明する。なお、このセンタ側処理は、書換装置20とセンタ30との間にデータ通信可能状態が確立されている状態において、例えば0.2秒というような所定時間間隔で実行されるものである。

【0081】

まず最初のステップS800において、アクセス拒否タイマが「0」か否かを判断する。アクセス拒否タイマは、後述するようにセンタ30によって書換装置20が「正当でない」と所定回数連続して判断された場合に設定されるものであ

る。ここでアクセス拒否タイマが「0」でないと判断された場合（S800：NO）、S810にてタイマをデクリメントし、さらに変数C2に「0」を代入して、本センタ側処理を終了する。変数C2は、センタ30にて書換装置20が正当でないと連続して判断された回数を計数するものである。一方、アクセス拒否タイマが「0」であると判断された場合（S800：YES）、S820へ移行する。

【0082】

S820では、変数C2が「2」以下であるか否かを判断する。ここで $C2 > 2$ である場合（S820：NO）、S830にてアクセス拒否タイマをセットし、その後、本センタ側処理を終了する。一方、 $C2 \leq 2$ である場合（S820：YES）、S840へ移行する。

【0083】

S840では、通信開始要求があったか否かを判断する。この処理は、図5中のS500の処理に対するものである。ここで通信開始要求があったと判断された場合（S840：YES）、S850へ移行する。一方、通信開始要求がない場合は（S840：NO）、この判断処理を繰り返す。

【0084】

S850では、書換装置20から送信されるID情報を受信し、発呼元の電話番号を取得する。続くS860では、受信したID情報と取得した電話番号との対応関係を、データベースに予め記憶された書換装置20のID情報と電話番号との対応関係と照合する。これらS850及びS860の処理が、図2中のB2に示した処理に相当する。

【0085】

そして、次のS870では、照合結果に基づき、対応関係が一致したか否かを判断する。ここで一致したと判断された場合（S870：YES）、S890にて第1許可信号及び関数fを送信し、その後、S900へ移行する。この処理が、図2中のB3の処理に相当する。一方、一致していないと判断された場合（S870：NO）、書き換えを許可しない旨を書換装置20へ通知すると共に、変数C2をインクリメントし（S880）、その後、S800からの処理を繰り返す。

す。

【0086】

なお、ここで説明した S 8 5 0 ~ S 8 9 0 までの処理が「正当性判断手段」としての処理に相当する。したがって、これらの処理を実行するセンタ 3 0 の C P U が「正当性判断手段」に相当する。

第 1 許可信号及び関数 f を送信した場合、書換装置 2 0 は、第 2 許可信号及び車両 V I N コードを送信してくるか（図 6 中の S 6 2 0）、あるいは書き換えの不許可を通知してくる（S 6 3 0）。

【0087】

そこで、S 9 0 0 では、書換装置 2 0 の応答があったか否かを判断する。ここで書換装置 2 0 の応答があったと判断された場合（S 9 0 0 : Y E S）、図 8 中の S 9 1 0 へ移行する。一方、書換装置 2 0 の応答がないうちは（S 9 0 0 : N O）、この判断処理を繰り返す。

【0088】

S 9 1 0 では、その応答が不許可の通知か否かを判断する。ここで不許可の通知であった場合（S 9 1 0 : Y E S）、図 7 中の S 8 0 0 へ移行する。一方、不許可の通知でない場合（S 9 1 0 : N O）、すなわち第 2 許可信号及び車両 V I N コードが送信された場合には、S 9 2 0 へ移行する。

【0089】

S 9 2 0 では、送信された車両 V I N コードに基づき車両の判別を行い、更新履歴のデータベースを参照する。そして、次の S 9 3 0 では、参照結果に基づき、制御情報を書き換える必要があるか否かを判断する。これら S 9 2 0 及び S 9 3 0 の処理が図 2 中の B 1 2 の処理に相当する。ここで書き換えの必要があると判断された場合（S 9 3 0 : Y E S）、S 9 5 0 へ移行する。一方、書き換えの必要がないと判断された場合（S 9 3 0 : N O）、S 9 4 0 にて書き換え済みを示す情報を送信し、その後、本センタ側処理を終了する。

【0090】

S 9 5 0 では、変更データを検索して読み出し、読み出した変更データを書換装置 2 0 へ送信する。この処理が、図 2 中の B 1 3 の処理に相当する。その後、

書換装置 20 からは、上述したように正常終了の通知（図 6 中の S700）あるいは異常終了の通知（S710）がなされる。

【0091】

したがって、S960 では、書換装置 20 からの終了通知があったか否かを判断する。ここで終了通知があったと判断された場合（S960：YES）、S970 へ移行する。一方、終了通知がないうちは（S960：NO）、この判断処理を繰り返す。

【0092】

S970 では、終了通知が正常終了の通知か否かを判断する。ここで正常終了の通知であると判断された場合（S970：YES）、S980 にて更新履歴のデータベースを更新し、その後、本センタ側処理を終了する。一方、正常終了の通知でないと判断された場合（S970：NO）、すなわち異常終了の通知であった場合には、S950 からの処理を繰り返す。

【0093】

次に、本実施例の制御情報書換システム 1 の発揮する効果を説明する。なお、ここでの説明に対する理解を容易にするため、最初に従来の問題点を簡単に説明する。

従来は図 9 に示したように、書換装置 200 の正当性を、ECU101～104 のみで判断していた。そして、この判断は、書換装置 200 に予め記憶されたアクセス情報としての関数 f に基づく通信開始処理（図 10 中の b1～b7）によって行われる。そのため、書換装置 200 又は書換装置 200 内部の情報が盗まれた場合、アクセス情報が盗まれるため、不正な制御情報の書き換えを防止することができなかった。

【0094】

これに対して、本実施例の制御情報書換システム 1 では、センタ 30 にアクセス情報としての関数 f を記憶しておき、センタ 30 が書換装置 20 を正当なものとして判断してはじめて、センタ 30 から書換装置 20 へ関数 f が送信される（図 2 中の B2，B3）。したがって、書換装置 20 又は書換装置 20 内部の情報が盗まれた場合であっても、書換装置 20 には ECU11～14 へのアクセス情

報が記憶されていないため、センタ 3 0 からアクセス情報を得ることができなければ、ECU 1 1 ~ 1 4 の制御情報を書き換えることはできない。

【0 0 9 5】

また、センタ 3 0 は、書換装置 2 0 にユニークに割り振られた ID 情報と電話回線を介してデータ通信を行う際の書換装置 2 0 側の電話番号とを対応させて記憶したデータベースを有している。そして、書換装置 2 0 から ID 情報を取得すると共に発呼元の電話番号を取得する（図 7 中の S 8 5 0）。この ID と電話番号との対応関係がデータベースに記憶された対応関係と一致している場合に（S 8 6 0, S 8 7 0 : Y E S）、センタ 3 0 は書換装置 2 0 が正当なものであると判断し、アクセス情報である関数 f を送信する（S 8 9 0）。例えば正規の作業場所以外からセンタ 3 0 との間に回線を接続した場合、センタ 3 0 の取得する電話番号は予め決められた電話番号でなくなる。そのため、ID 情報と対応せず、センタ 3 0 からアクセス情報を得ることはできない。結果として、ECU 1 1 ~ 1 4 の制御情報を書き換えることはできない。

【0 0 9 6】

以上のように、本実施例の制御情報書換システム 1 によれば、書換装置 2 0 又は書換装置 2 0 内部の情報が盗まれた場合であっても、ECU 1 1 ~ 1 4 の制御情報が不正に書き換えられることを確実に防止できる。

そして、本実施例の制御情報書換システム 1 では、センタ 3 0 が最初に書換装置 2 0 の正当性を判断し、続いて ECU 1 1 ~ 1 4 が書換装置 2 0 の正当性を判断する。これら 2 段階のチェックのいずれにおいても、書換装置 2 0 が「正当でない」と連続して 3 回判断された場合、1 0 分間のアクセス拒否を行うようにした。

【0 0 9 7】

すなわち、ECU 1 1 ~ 1 4 では、書換装置 2 0 を正当でないと判断すると（図 4 中の S 3 8 0 : N O）変数 C 1 をインクリメントし（S 4 1 0）、変数 C 1 が「2」よりも大きくなると（図 3 中の S 3 3 0 : N O）、すなわち 3 回連続して「正当でない」との判断がなされると、アクセス拒否タイマを設定する（S 3 4 0）。これによって、タイマが「0」となるまで書換装置 2 0 のアクセスを拒

否する（S 3 1 0 : N O）。

【0 0 9 8】

一方、センタ 3 0 でも同様に、書換装置 2 0 を正当でないと判断すると（図 7 中の S 8 7 0 : N O）、変数 C 2 をインクリメントしていき（S 8 8 0）、変数 C 2 が「2」よりも大きくなると（S 8 2 0 : N O）、すなわち 3 回連続して「正当でない」との判断がなされると、アクセス拒否タイマを設定する（S 8 3 0）。これによって、タイマが「0」となるまで書込装置 2 0 のアクセスを拒否する（S 8 0 0 : N O）。

【0 0 9 9】

その結果、不正な情報を用いてセンタ 3 0 や E C U 1 1 ~ 1 4 を書換装置 2 0 からアクセスしようとしても、連続して何度もアクセスすることができないため、本実施例では 3 回続けて不正なアクセスを行えば 1 0 分間アクセスができなくなるため、制御情報の書き換え防止に有効である。

【0 1 0 0】

また、本実施例の制御情報書換システム 1 では、センタ 3 0 が制御情報の変更データを記憶している。すなわち、従来のように書換装置 2 0 に変更データを記憶しておかないため、書換装置 2 0 又は書換装置 2 0 内部の情報が盗まれた場合であっても、変更データが外部に漏れる可能性がない。

【0 1 0 1】

そして、センタ 3 0 は、E C U 1 1 ~ 1 4 からの第 2 許可信号が送信されてきたことを一つの条件として（S 9 1 0 : N O）変更データを送信する（S 9 5 0）。すなわち、E C U 1 1 ~ 1 4 にて書換装置 2 0 が正当であると判断されたことを条件として変更データを送信する。したがって、変更データが外部に漏れる可能性をさらに低減させている。

【0 1 0 2】

さらに、E C U 1 1 ~ 1 4 は、書換装置 2 0 を正当であると判断すると（図 4 中の S 3 8 0 : Y E S）、上述した第 2 許可信号に加え、車両 1 0 を特定可能な車両 V I N コードを送信する（S 3 9 0）。センタ 3 0 は、各車両 1 0 の E C U 1 1 ~ 1 4 に記憶された制御情報更新履歴のデータベースを有しており、上述し

た ECU 1 1 ~ 1 4 から車両 V I N コードに基づき、車両 1 0 を判別しこのデータベースを参照して（図 8 中の S 9 2 0）制御情報の書き換えの必要性を判断する（S 9 3 0）。そして、書き換えの必要がある場合に（S 9 3 0 : Y E S）変更データを送信する（S 9 5 0）。

【 0 1 0 3 】

従来は、過去に ECU 1 1 ~ 1 4 の制御情報が書き換えられているか否かを判断できない状況があった。そのため、制御情報のバージョンアップの履歴がない場合には、既に制御情報の書き換えが行われているにもかかわらず、再度制御情報の書き換えを行うというような無駄な制御情報の書き換えが行われていた。このような場合、無駄な作業時間を要するだけでなく、例えば制御情報の記憶に E P R O M を用いている場合、書き換え可能回数が制限されるため、無駄な書き換えによって必要な書き換えができなくなるおそれもあった。

【 0 1 0 4 】

これに対して、本実施例では、上述したようにセンタ 3 0 が各車両 1 0 の制御情報の更新履歴を管理するため、無駄な制御情報の書き換えが行われない。その結果、無駄な作業時間がなくなり、また、無駄な書き換えによって必要な書き換えができなくなることもなくなる。

【 0 1 0 5 】

さらにまた、本実施例の制御情報書換システム 1 のセンタ 3 0 では、ECU 1 1 ~ 1 4 から書換装置 2 0 を経由して書き換えの正常終了が通知されると（図 8 中の S 9 7 0 : Y E S）、自動的に制御情報の更新履歴のデータベースを更新する（S 9 8 0）。したがって、作業者がマニュアル操作でデータベースを更新する必要がなく便利である。

【 0 1 0 6 】

また、本実施例の制御情報書換システム 1 の書換装置 2 0 では、アクセス情報としての関数 f が必要なくなると（図 6 中の S 6 5 0 : N O, S 6 9 0 : Y E S）、速やかにそのアクセス情報である関数 f を抹消する（S 6 6 0, S 7 0 0）。そのため、センタ 3 0 から書換装置 2 0 へ送信されたアクセス情報としての関数 f が書換装置 2 0 から盗まれる可能性を低減させることができる。

【0107】

以上、本発明はこのような実施例に何等限定されるものではなく、本発明の主旨を逸脱しない範囲において種々なる形態で実施し得る。

(1) 上記実施例においては、センタ30が書換装置20から発呼され、その後、センタ30と書換装置20との間にデータ通信可能状態が確立されると、センタ30は、対応情報として発呼元の電話番号を取得し、書換装置20から送信される識別情報としてのID情報との対応によって、書換装置20の正当性を判断していた。

【0108】

これに対して、センタ30が書換装置20のID情報とパスワードとを対応させたデータベースを有する構成とし、書換装置20は、作業者によって入力されるパスワードを、上述したID情報と共に送信する構成としてもよい。この場合、パスワードが「対応情報」に相当することになり、センタ30は、書換装置20から送信されるID情報とパスワードとの対応によって、書換装置20の正当性を判断する。

【0109】

また、上記実施例では、書換装置20に予めID情報が記憶されていたが、ID情報も、パスワードと同様に利用者から入力されるようにしてもよい。

このようにすれば、書換装置20又は書換装置20内部の情報が盗まれた場合であっても、パスワード、あるいは、ID情報及びパスワードが分からないため、センタ30からアクセス情報を得ることはできず、上記実施例と同様に制御情報の不正な書き換えを防止することができる。

【0110】

ただし、ID情報やパスワードが何らか別のルートで盗まれる可能性もあるため、上記実施例のように書換装置20の設置場所に関連する電話番号を対応情報とすることがより好ましい。不正な書き換えは正規の作業現場では行われなためである。

【0111】

(2) また、書換装置20がセンタ30からアクセス情報を取得した後、セン

タ 3 0 と書換装置 2 0 との間のデータ通信を一時的に終了することが考えられる。例えば、図 2 中の B 1 ～ B 4 の通信処理が終了した後に一旦データ通信を終了し、B 1 1 以降の処理を行う際に、書換装置 2 0 とセンタ 3 0 との間にデータ通信可能状態を再度確立することが考えられる。

【 0 1 1 2 】

ただし、書換装置 2 0 に送信されたアクセス情報が盗まれ、別の書換装置を用い、このアクセス情報を使用して E C U 1 1 ～ 1 4 がアクセスされる可能性がある。

したがって、一連の書き換え処理（図 2 に示す B 1 ～ B 1 8 の処理）が終了するまで、センタ 3 0 と書換装置 2 0 がデータ通信可能状態となっていることを書き換えの条件とするとよい。

【 0 1 1 3 】

具体的には次のように構成することが考えられる。それは、書換装置 2 0 がタイム割込処理などによって定期的にセンタ 3 0 へ応答要求を送信し、センタ 3 0 が応答を行う構成とする。このとき、一連の書き換え処理が完了する前にセンタ 3 0 からの応答がなくなった場合、書換装置 2 0 が E C U 1 1 ～ 1 4 の書き換えを行わないようにする。このようにすれば、盗んだアクセス情報を用いて別の書換装置から E C U をアクセスすることができなくなる。

【図面の簡単な説明】

【図 1】 実施例の制御情報書換システムの構成を示すブロック図である。

【図 2】 実施例における書き換え処理の概要を示す説明図である。

【図 3】 E C U 側処理の前半部分を示すフローチャートである。

【図 4】 E C U 側処理の後半部分を示すフローチャートである。

【図 5】 書換装置側処理の前半部分を示すフローチャートである。

【図 6】 書換装置側処理の後半部分を示すフローチャートである。

【図 7】 センタ側処理の前半部分を示すフローチャートである。

【図 8】 センタ側処理の後半部分を示すフローチャートである。

【図 9】 従来の制御情報書換システムの構成を示すブロック図である。

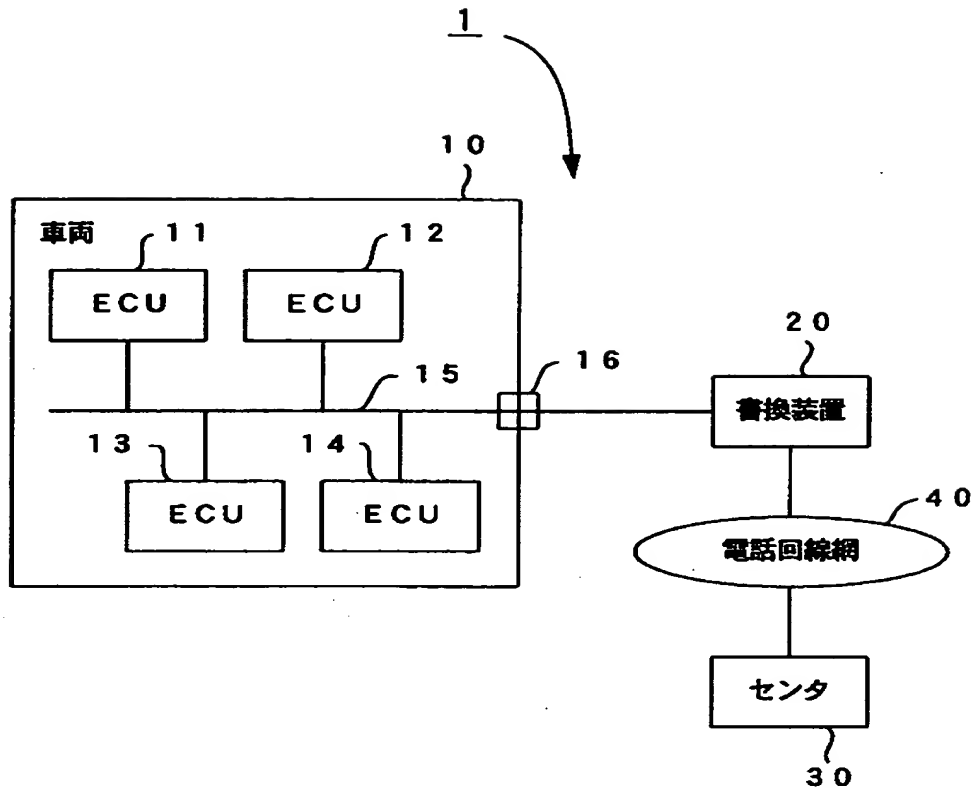
【図 10】 従来の書き換え処理の概要を示す説明図である。

【符号の説明】

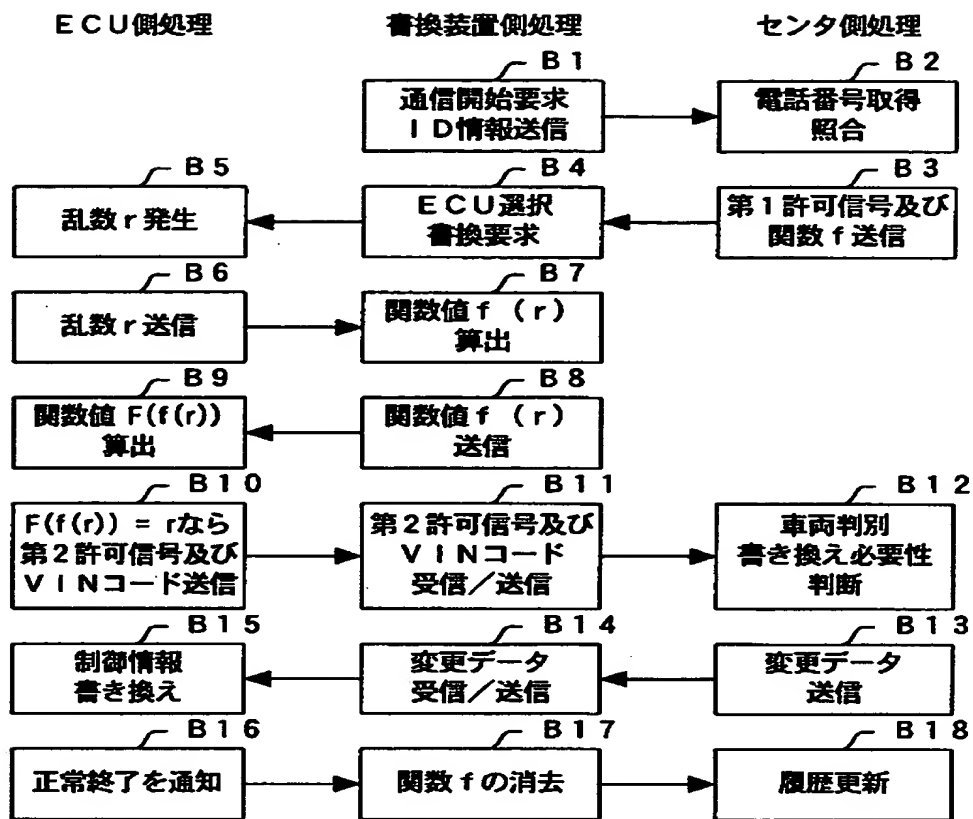
- 1 …制御情報書換システム
- 1 1, 1 2, 1 3, 1 4 …E C U
- 1 5 …ネットワーク回線
- 1 6 …車両ダイアグコネクタ
- 2 0 …書換装置
- 3 0 …センタ
- 4 0 …電話回線網

【書類名】 図面

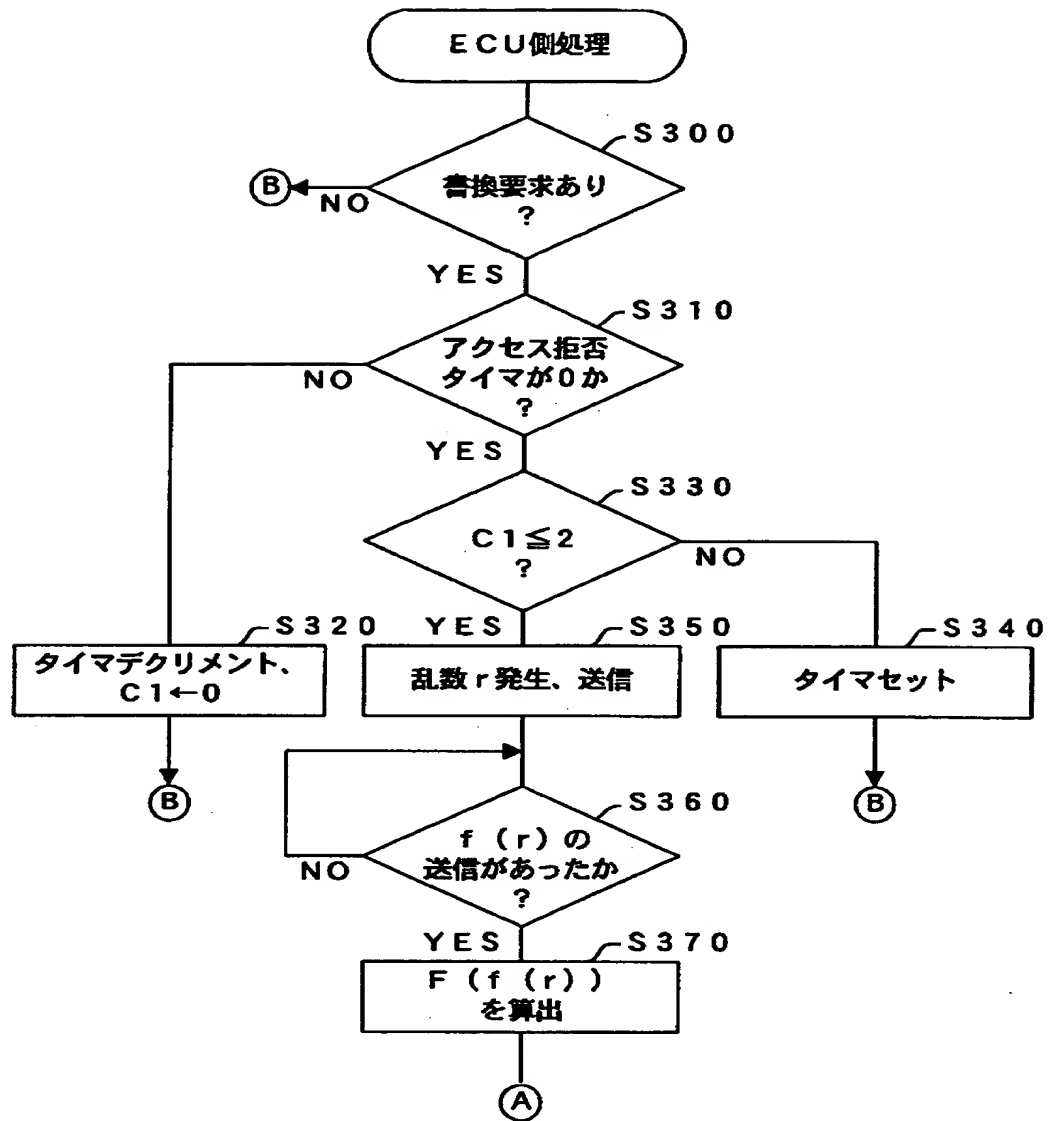
【図 1】



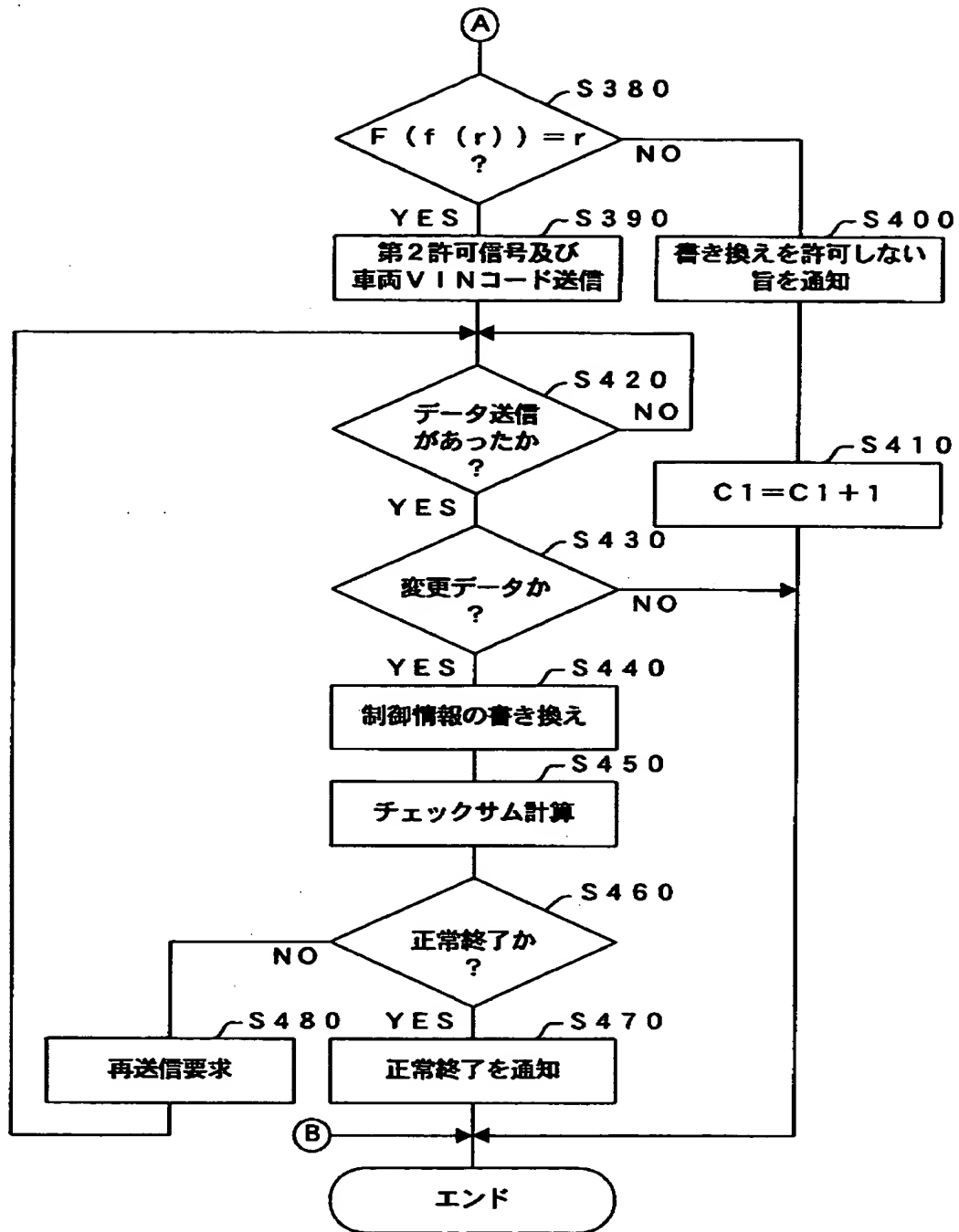
【図 2】



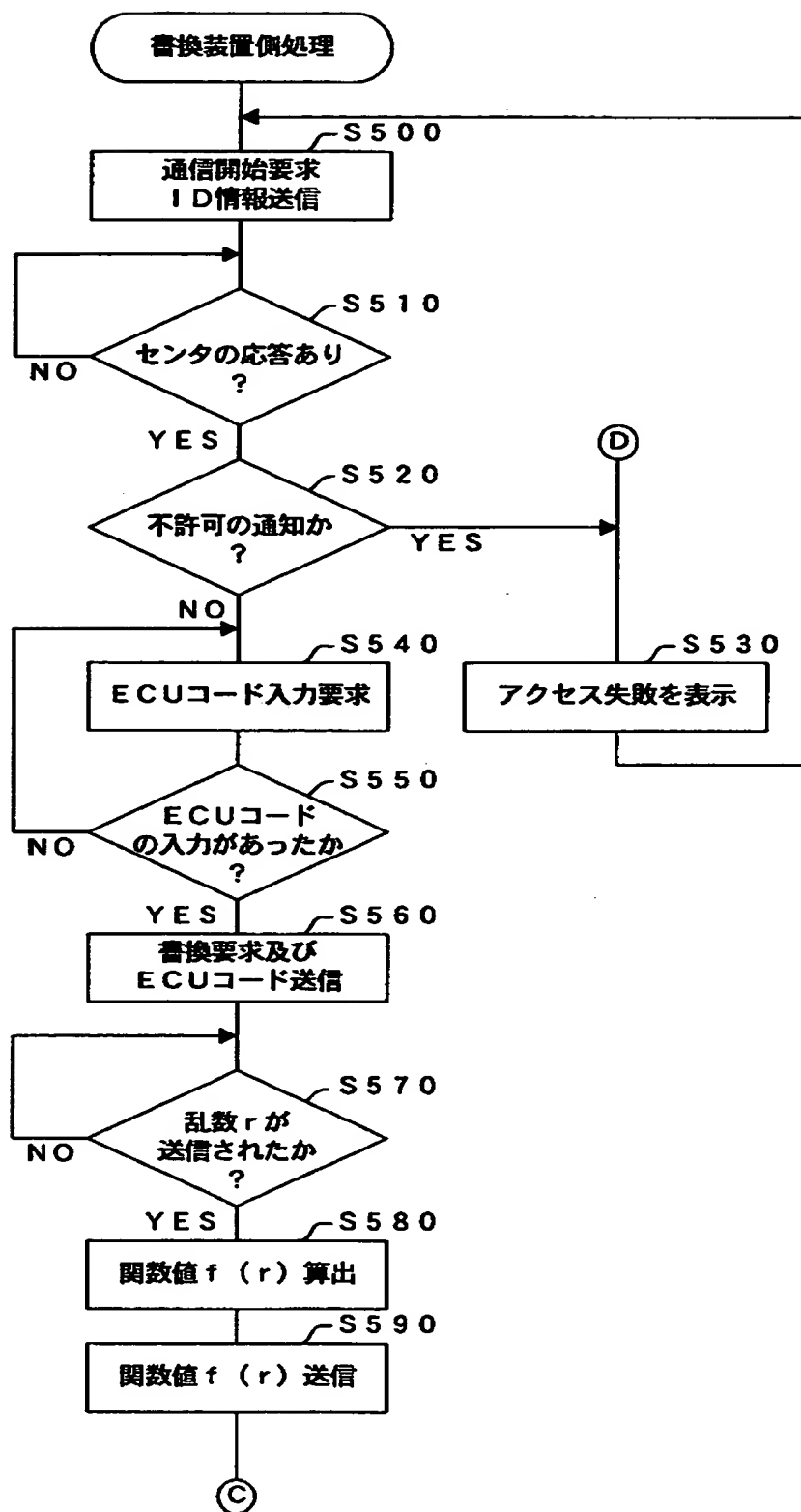
【図 3】



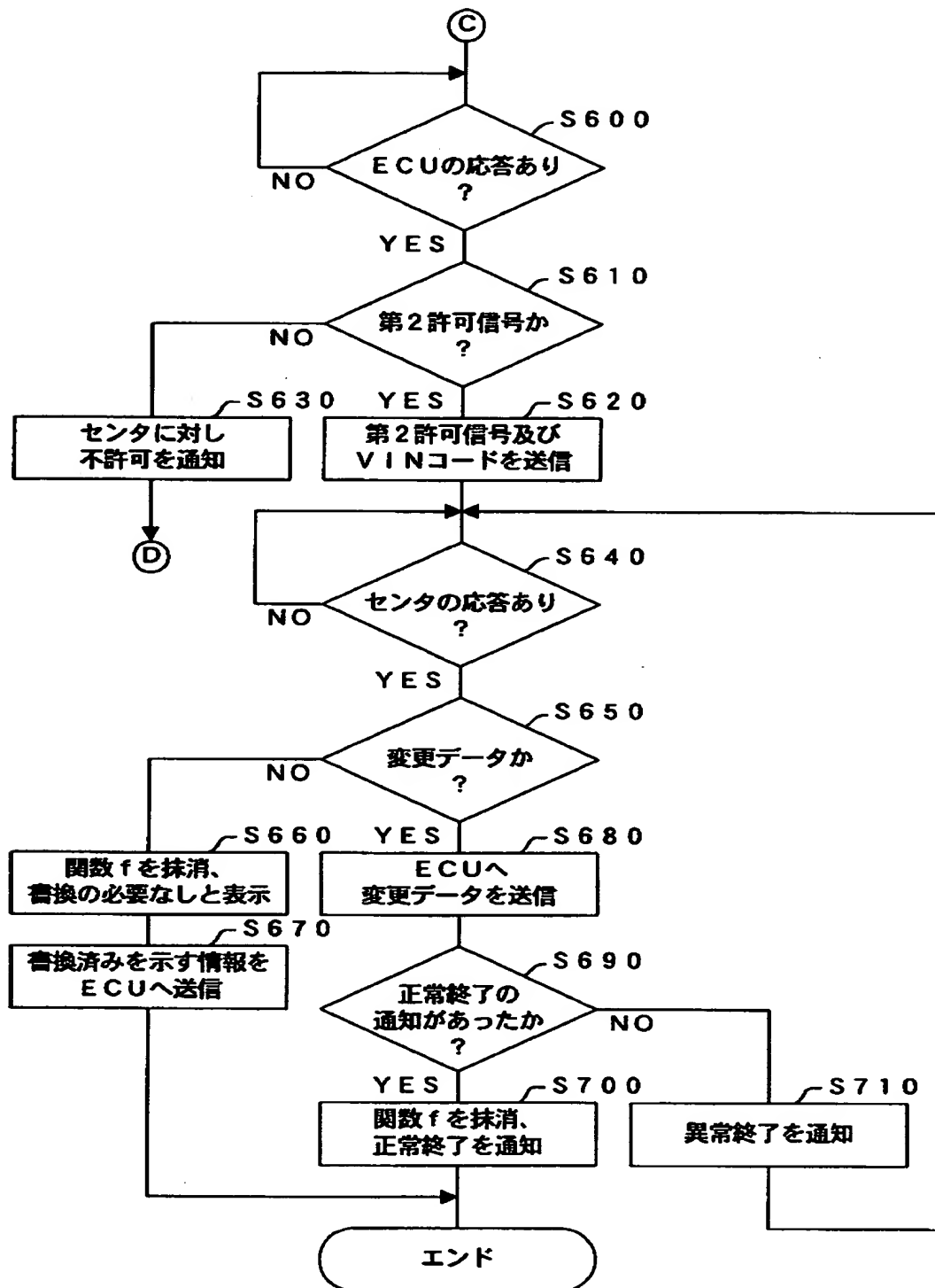
【図 4】



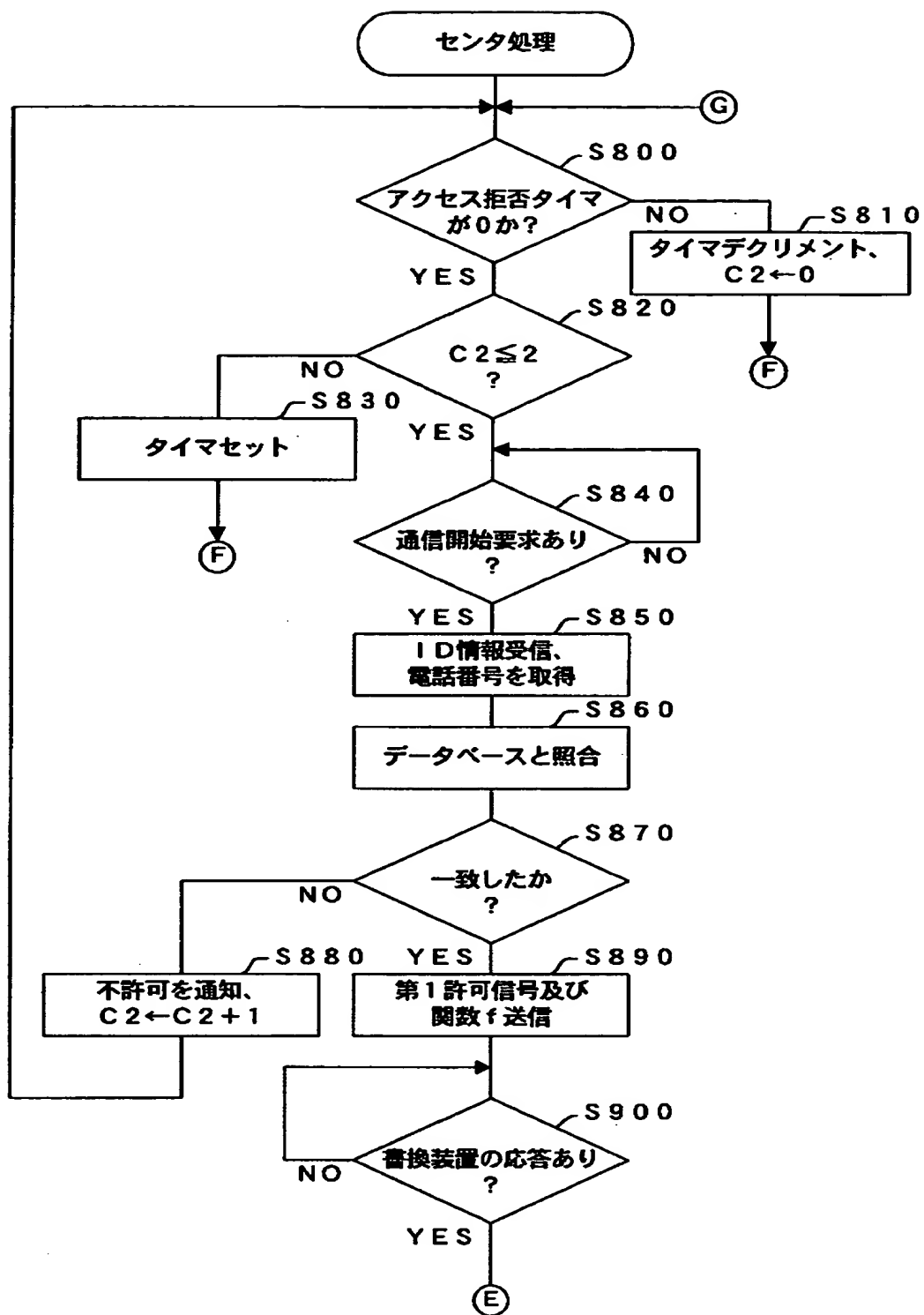
【図 5】



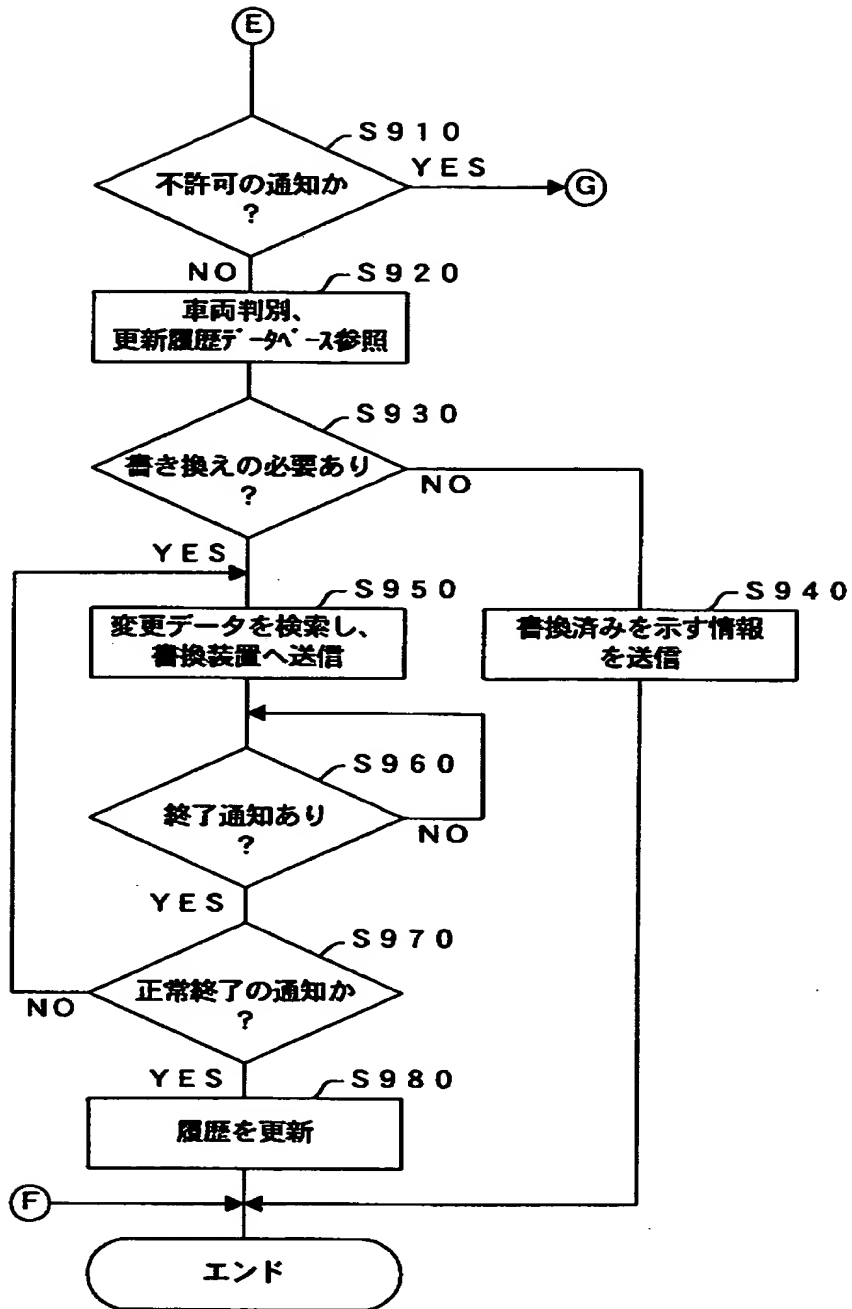
【図 6】



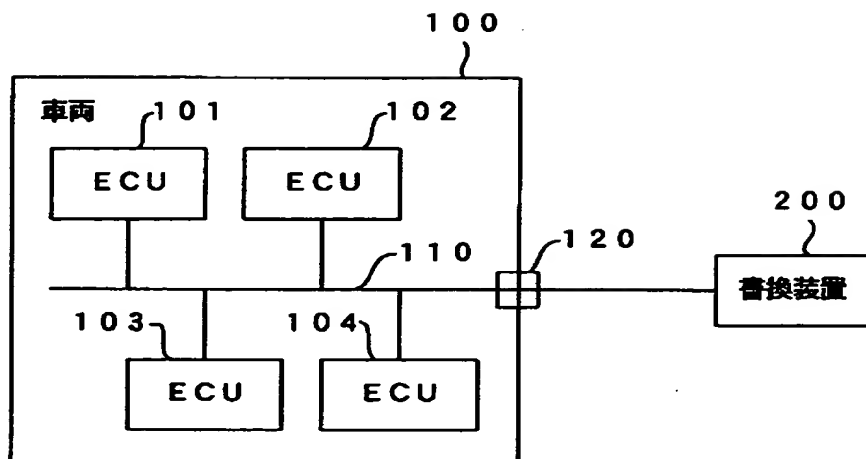
【図 7】



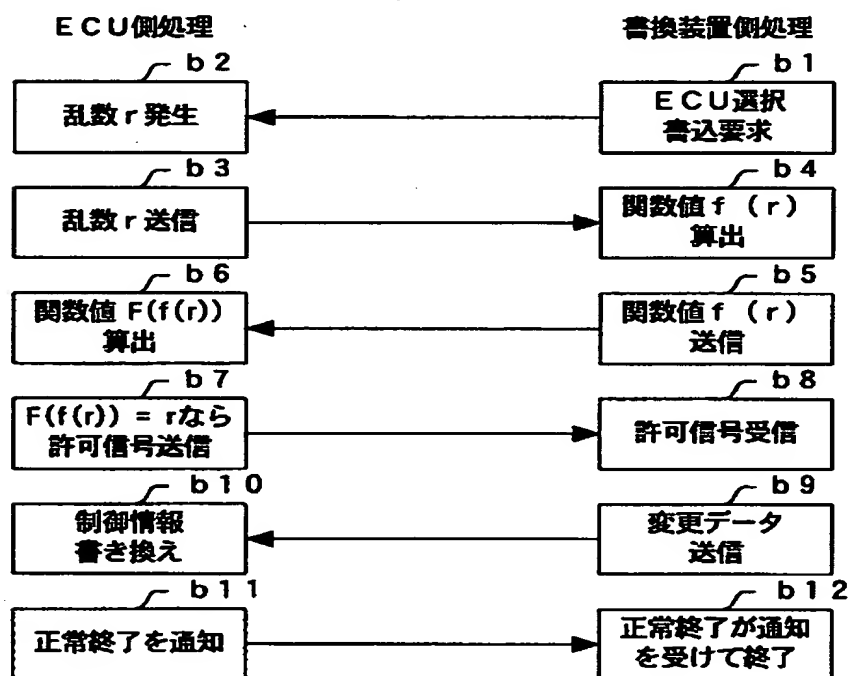
【図 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 書換装置又は書換装置内部の情報が盗まれた場合であっても、電子制御装置における制御情報の不正な書き換えを防止できるようにする

【解決手段】 書換装置 2 0 が ECU 1 1～1 4 にアクセスするために必要な関数 f をセンタ 3 0 に記憶しておく。そして、センタ 3 0 は、書換装置 2 0 を正当なものと判断してはじめて、書換装置 2 0 へ関数 f を送信する。センタ 3 0 は、書換装置 2 0 に対しユニークに割り振られた I D 情報と電話回線網 4 0 を介してデータ通信を行う際の書換装置 2 0 側の電話番号とを対応させて記憶したデータベースを有している。そして、書換装置 2 0 から I D 情報を取得すると共に発呼元の電話番号を取得し、この I D と電話番号との対応関係がデータベースに記憶された対応関係と一致している場合に、書換装置 2 0 を正当なものと判断する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000004260]

1. 変更年月日	1996年10月 8日
[変更理由]	名称変更
住 所	愛知県刈谷市昭和町1丁目1番地
氏 名	株式会社デンソー